(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 719 045 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
29.10.2003 Bulletin 2003/44

(51) Int Cl.[7]: **H04N 7/167**

(21) Application number: **95119605.4**

(22) Date of filing: **13.12.1995**

(54) **Crypt key system for secure electronic transactions**

Verschlüsselungssystem für sichere elektronische Transaktionen

Système de cryptage pour des transactions électroniques sécurisées

(84) Designated Contracting States:
DE FR GB

(30) Priority: **13.12.1994 JP 30929294**

(43) Date of publication of application:
26.06.1996 Bulletin 1996/26

(73) Proprietor: **MITSUBISHI CORPORATION**
Chiyoda-ku, Tokyo 100-0005 (JP)

(72) Inventor: **Saito, Makoto**
Tama-shi, Tokyo (JP)

(74) Representative: **Pfenning, Meinig & Partner**
Mozartstrasse 17
80336 München (DE)

(56) References cited:
EP-A- 0 438 154 **EP-A- 0 450 841**
EP-A- 0 506 435

- **CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993, no. SYMP. 18, 11 June 1993, POSTES;TELEPHONES ET TELEGRAPHES SUISSES, pages 761-769, XP000379391 VIGARIE J P: "A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER"**

EP 0 719 045 B1

Description

Background of the Invention

Field of the Invention

[0001] The present invention relates to a crypt key system that is used in a commercial trade or the like which uses a television system, a database system or an electronic data interchange.

Prior Art

[0002] In the information oriented society of today, in addition to a normal terrestrial broadcasting, satellite broadcasting which is referred to as a broadcasting satellites (BS) and communication satellites (CS), or cable TV broadcasting, which is referred to as CATV (cable television) using coaxial cables or optical cables, is getting prevalent.

[0003] In a satellite broadcasting or CATV broadcasting which distributes several tens of channels at the same time, scrambled channels of such as films, sport events, and music which cannot be viewed through comprehensive contracts are provided in addition to unscrambled general channels. In order to view these channels, it is necessary to subscribe to descramble the channels; however, a normal subscription period is about one-month unit, and it is impossible to view through temporary contracts.

[0004] The inventor of the present invention proposed in the Japanese Patent Application Laid-Open No. JP-A-6-046419 (see also corresponding GB-A-2 269 302) and the Japanese Patent Application Laid-Open No. JP-A-6-141004 (see also corresponding US-A-5 504 933) a system in which users obtain a viewing permit key from a charging center via a communication line and charged, and descrambles programs scrambled each by respectively different scramble pattern, using the viewing permit key to view the programs; proposed in the Japanese Patent Application Laid-Open No. JP-A-6-132916 (see also corresponding GB-A-2 272 822) an apparatus for the operation.

[0005] In these system and apparatuses, those who wish to use scrambled programs make a request for viewing to the charging center via a communication line by using a communication apparatus. The charging center transmits the viewing permit key to the communication apparatus corresponding to the request for viewing while charging and collecting a fee.

[0006] Users, on receiving the viewing permit key with the communication apparatus, transmit the viewing permit key to the receiving apparatus via direct means connecting the communication apparatus and the receiving apparatus or via indirect means such as flexible disks or the like. The receiving apparatus to which the viewing permit key is transmitted descrambles the programs with the viewing permit key and then the users use the programs.

[0007] Said Japanese Patent Application Laid-Open No. JP-A-6-132916 describes a system and an apparatus for selling and renting of a tape or a disk on which a plurality of data scrambled with a respective plurality of different scramble patterns are recorded to supply the viewing permit key with IC cards or the like and use specific data.

[0008] In addition, in these days of an information-oriented society, a database system has been propagated for mutually using data which are kept independently by each of computers constituting a computer communication network by LAN (local area network), WAN (wide area network), and Inter-Net system mutually connecting these networks.

[0009] In the meantime, a technology has been developed for reducing the information amount by compressing a television moving picture signal which could not be digitized because of a huge amount of information as a result of digitization, to enable practical digitization. So far, the H.261 standard for video conference, the JPEG (joint photographic image coding experts group) standard for static pictures, the MPEG 1 (moving picture image coding experts group 1) standard for storing pictures and MPEG 2 corresponding to the present telecast and the high-definition telecast from the television broadcasting are prepared.

[0010] The digitization technology using these picture compression technology is used for the television broadcasting or the video picture recording. In addition, even television moving picture data which could not be dealt with before can be dealt with now. Then, the "multimedia system" which deals with various data dealt with by the computer and the digitized television moving picture data has been focused as a future technology.

[0011] This multimedia system is also incorporated in the data communication and can be used as one data on the database.

[0012] While the scope of usage of the database is expanded, the method for charging for the data usage on the database, and the method for dealing with copyright problems generated by copying, transmitting other than direct usage of data, and also the secondary exploitation right problem generated as a result of data edition have become important problems.

[0013] To safely deal with charging and copyrights processes, it is required that the data cannot be used by users other than authorized users, and data encryption is the best means for it.

[0014] In addition, an electronic market system has been investigated for converting information in various kinds of transactions which have been carried out by paper documents so far, into electronic data to execute electronic transactions by using the electronic data interchange for transmitting and receiving data by the data communication technology. In addition, an investigation is also made on the possibility of carrying out an electronic settlement on the electronic commercial transac-

tion system.

[0015] In the commercial transactions, reliability on the transaction details is required and security in the settlement is required. Consequently, in the electronic commercial transaction system and electronic settlement system in which such reliability and security are demanded, it is required that the data is encrypted so that the data will not be falsified or used unjustifiedly.

[0016] In these television systems, database systems or electronic commercial transaction systems or the like, the data is encrypted and thus a crypt key is required for decrypting the encrypted data to use. And the crypt key must be given to data users; however, the processing is very troublesome because security and reliability are demanded.

[0017] In the structure of the present invention, data cryptology acts an important part. In the beginning, a general explanation will be made on data cryptology.

[0018] EP-A-0 506 435 discloses a crypt key system in which a key used in scrambling program data is twice encrypted and multiplexed with the scrambled signal.

[0019] In data cryptology, the case in which the plaintext data M is encrypted by using a crypt key K to obtain cryptogram data C is represented as:

$$C=E(K, M),$$

and the case in which the cryptogram data C is decrypted by using the crypt key K to obtain the plaintext data M is represented as:

$$M=D(K, C).$$

[0020] As a typical method for the data cryptography technology, there are a secret-key cryptosystem and a public-key cryptosystem. The secret-key cryptosystem is a cryptosystem in which same secret key Ks is commonly used in encryption and decryption:

$$Cmks=E(Ks, M)$$

$$M=D(Ks, Cmks).$$

[0021] The public-key cryptosystem is a cryptosystem in which a key for encryption and a key for decryption are used as crypt keys, and the key for encryption is laid open but the key for decryption is not open. The key for encryption is referred to as a public-key Kb while the key for decryption is referred to as a private-key Kv. To use this cryptosystem, an information sender encrypts the plaintext data M by the public-key Kb of a receiver

$$Cmkb=E(Kb, M),$$

and the receiver receives the data and decrypts it by a private-key Kv to obtain the plaintext data M

$$M=D(Kv, Cmkb).$$

[0022] In this public-key cryptosystem, cryptanalysis is very difficult.

[0023] As an application of the data cryptography technology, a digital signature process is performed as an electronic data authentication means to ensure the reliability of the data.

[0024] The digital signature process is used with a secret-key system or a public-key system. Generally, the public-key system is used with the digital signature.

[0025] In the digital signature process which is carried out by using the public-key system, the signer obtains a digital signature by encrypting a document m to which the document M is compressed with a hash algorithm, using the private-key Kv of the signer:

$$Smkv=E(Kv, m)$$

and transmits the original document M or the compressed document m and the digital signature Smkv to the receiver.

[0026] The receiver decrypts the digital signature Smkv by using the public-key Kb of the signer

$$m'=D(Kb, Smkv).$$

When m'=m is established, it is recognized that the signature is correct.

[0027] EP-A-0 438 154 discloses a multimedia network system in which payload data are transmitted encrypted by a secret key, and wherein a public key system is used for exchanging the secret key between the communicating parties.

[0028] As a method for providing these crypt keys to users, the inventor of the present invention proposed an invention entitled "crypt key system" in the prior Japanese Patent Application No. 6-70643 (filed 08.04.1994 and published under JP-A-7 283 809 and corresponding EP-A-0 676 897).

[0029] In the generally practiced crypt key system, the crypt key is provided only to users while the crypt key is provided to persons other than the users in the crypt key system of this prior invention.

[0030] Fig. 1 shows the structure of the crypt key system proposed in the Japanese Patent Application No. 6-70643.

[0031] This system comprises a broadcasting station 1 for multiplex broadcasting such as BS, CS, terrestrial broadcasting or FM or the like or data broadcasting, a database 2, a charging center 3, a receiving apparatus 4, data communication apparatus 5 and a user's termi-

nal 8.

[0032] The broadcasting station 1 and the database 2, and the database 2 and the charging center 3 are connected to each other via a communication line such as a dedicated line or the like or flexible disc or the like. The database 2 and the data communication apparatus 5 are connected by a communication line 7 such as a communication line or CATV line.

[0033] The broadcasting station 1 and the receiving apparatus 4 are connected with the broadcasting radio wave 6. The receiving apparatus 4 and the user terminal apparatus 8, and the data communication apparatus 5 and the user terminal 8 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc.

[0034] In Fig. 1, what is shown with a solid line is a path of information which is not encrypted. What is shown with a broken line is a path of data which is encrypted.

[0035] In this system, the database 2 preliminarily supplies a permit key Kp (hereinafter referred to as a "permit key") including the crypt key Kd which is different from one data to another to the broadcasting station 1. The permit key Kp is explained in such a manner that the permit key Kp constitutes the crypt key Kd only for better understanding.

[0036] In some cases, the crypt key Kd is supplied without being encrypted, and in other cases, it is encrypted by using a common crypt key KO

$$Ckdk0=E\ (KO,\ Kd),$$

and is supplied as an encrypted crypt key Ckdk0.

[0037] In the case where the crypt key Kd is encrypted and supplied, a common crypt key K0 for decrypting the encrypted crypt key Ckdk0 is supplied to users. This common crypt key K0 is supplied when users register with the database, or it is supplied to the users together with the encrypted data Cmkd when the encrypted data Cmkd is transmitted.

(a) In the case where the crypt key is not encrypted:

[0038] In this crypt key system, the broadcasting station 1 broadcasts the crypt key Kd supplied from the database 2, by using the radio wave 6.

[0039] The receiving apparatus 4 supplies the received crypt key Kd to the user terminal 8 so that the user terminal 8 stores the received crypt key Kd in a recording medium such as a semiconductor memory, a flexible disc, a hard disc or the like.

[0040] The users who wish to use data make a request for the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

[0041] The database 2 which has received the request for the data M encrypts the data M by the crypt key Kd which is a permit key Kp

$$Cmkd=E\ (Kd,\ M),$$

and transmits the encrypted data Cmkd to the data communication apparatus 5 of users via the communication line 7 and charges the user with the charging center 3.

[0042] The data communication apparatus 5 supplies the received encrypted data Cmkd to the user terminal 8 while the user terminal 8 decrypts the encrypted data Cmkd by the crypt key Kd which is stored in the recording medium

$$M=D\ (Kd,\ Cmkd).$$

(b) In the case where the crypt key is encrypted and the common crypt key is preliminarily distributed to users:

[0043] In this crypt key system, when users register to use the database, the common crypt key K0 is supplied to the users with a recording medium such as ROM or flexible disc and the supplied common crypt key K0 is stored in the user terminal 8.

[0044] The database 2 encrypts the crypt key Kd by using the common crypt key KO

$$Ckdk0=E\ (K0,\ Kd),$$

and supplies the encrypted crypt key Ckdk0 to the broadcasting station 1.

[0045] The broadcasting station 1 broadcasts the received encrypted crypt key Ckdk0 supplied from database 2 by using the radio wave 6.

[0046] The receiving apparatus 4 supplies die received encrypted crypt key Ckdk0 to the user terminal 8 which decrypts the encrypted crypt key Ckdk0 in the beginning by the preliminarily stored common crypt key K0

$$Kd=D\ (K0,\ Ckdk0),$$

and stores the decrypted crypt key Kd in a recording medium such as a semiconductor memory, a flexible disc or a hard disc.

[0047] Users who wish to use data make requests for the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

[0048] The database 2 which receives a request for the data encrypts the requested data M by the crypt key Kd

$$Cmkd=E\ (Kd,\ M),$$

and transmits it to the data communication apparatus 5 via the communication line 7 and charges the user with the charging center 3.

[0049] The data communication apparatus 5 supplies the received encrypted data Cmkd to the user terminal 8 which decrypts the encrypted data Cmkd by the stored crypt key Kd

$$M=D(Kd, Cmkd).$$

(c) In the case where the crypt key is encrypted and the common crypt key is distributed to the user together with the encrypted data:

[0050] In this crypt key system, the database 2 encrypt the crypt key Kd by the common crypt key K0

$$Ckdk0=E(K0, Kd)$$

and supplies it to the broadcasting station 1.

[0051] The broadcasting station 1 broadcasts the encrypted crypt key Ckdk0 which has been supplied from the database 2, by using the radio wave 6.

[0052] The receiving apparatus 4 supplies the received encrypted crypt key Ckdk0 to the user terminal 8. The user terminal 8 stores the encrypted crypt key Ckdk0 in a recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

[0053] Users who wish to use data make a request for the data M to the database 2 via the communication line 7 by using the data communication apparatus 5.

[0054] The database 2 which receives the request for the data encrypts the requested data M by the crypt key Kd

$$Cmkd=E(Kd, M),$$

and transmits it to the data communication apparatus 5 via the communication line 7 together with the common crypt key K0 and charges the user with the charging center 3.

[0055] The data communication apparatus 5 supplies the received encrypted data Cmkd and the common crypt key K0 to the user terminal 8. The user terminal 8 decrypts the encrypted crypt key Ckdk0 which has been stored in the recording medium by the common crypt key K0

$$Kd=D(K0, Ckdk0),$$

and decrypts the encrypted data Cmkd by the decrypted crypt key

$$Kd\ M=D(Kd, Cmkd).$$

Summary of the Invention

[0056] The problem of the present invention is to provide a crypt key system which prevents unjustified use of a database system, in a pay-per-view system or a video-on-demand system. This problem is solved by a crypt key system according to claim 1. Further improvement of the crypt key system of claim 1 is provided in the dependent claim.

[0057] This system comprises a broadcasting station, a database, a receiving apparatus, a data communication apparatus, and a user terminal. As crypt key systems, a secret-key cryptosystem and a public-key cryptosystem are used. In addition, a digital signature may be used, and the crypt key is supplied through broadcasting.

[0058] The present invention is a useful means in the realization of a database system, a pay-per-view system or a video-on-demand system, an electronic market using an electronic data interchange system.

Brief Description of the Drawings

[0059]

Fig. 1 is a structural view of a crypt key system according to the prior applications.

Fig. 2 is a structural view of the crypt key system according to a first embodiment of the present invention.

Embodiments

[0060] Embodiments of the present invention will be described by using Fig. 2.

[Embodiment 1]

[0061] A system shown in Fig. 2 is a crypt key system of the embodiment in which the present invention is applied to a database system. This system comprises a broadcasting station 11 with either a multiplex broadcasting of BS, CS, a terrestrial wave television, or FM broadcasting or the like, or data broadcasting by a digital broadcasting, a database 12 in which various kinds of data including moving picture data is stored, a charging center 13, a receiving apparatus 14 for receiving the data broadcasting offered by the broadcasting station 11, a data communication apparatus 15 for communicating with the database 12 and a user terminal 18 for using the data.

[0062] The database 12 and the broadcasting station 11, and the database 12 and the charging center 13 are connected with a direct means connecting with a com-

munication line such as a dedicated line or an indirect means such as a flexible disc or the like. The database 12 and the data communication apparatus 15 connected with a communication line 17 such as a communication line, or CATV line or the like. Then, the broadcasting station 11 and the receiving apparatus 14 are connected with a radio wave 16 such as a terrestrial wave television broadcasting, satellite television broadcasting, CATV broadcasting, FM broadcasting or a satellite data broadcasting or the like. The receiving apparatus 14 and the user terminal 18, and the data communication apparatus 15 and the user ,terminal 18 are connected with a direct means such as a connection cable or an indirect means such as a flexible disc or the like.

[0063] What is shown with a solid line in Fig. 2 is an uncrypted data path and what is shown with a broken line is an encrypted data path.

[0064] Incidentally, data exchange between the database 12 and the broadcasting station 11, and the database 12 and the charging center 13 are, in principle, carried out with a dedicated line or a flexible disc. In addition, a public line, a broadcasting satellite, a communication satellite or a terrestrial wave broadcasting can be used. In such a case, the data is encrypted.

[0065] In this system, the secret-key cryptosystem and the public-key cryptosystem are used.

[0066] The database 12 prepares the public-key Kbd and the private-key Kvd to supply the public-key Kbd to the broadcasting station 11. The broadcasting station 11 which receives the public-key Kbd broadcasts it by a teletext multiplexing broadcasting using scanning lines during the retrace blanking interval period of an analog television picture signal, the data broadcasting using a sub audio band of the analog television audio signal, FM multiplex data broadcasting or digital data broadcasting.

[0067] Further, in this case, a digital signature of the database 11 can be added to the public-key Kbd.

[0068] The data may be supplied without encrypting the menu, the titles of data which can be used, the content introduction of the data, product catalogs, order forms, blank checks and/or the copyright information for the convenience of the data usage.

[0069] The receiving apparatus 14 which receives the transferred public-key Kbd sends the public-key Kbd to the user terminal 18. The user terminal 18 which receives the transferred public-key Kbd stores the public-key Kbd in a recording medium such as a semiconductor memory, a flexible disc, or a hard disc or the like.

[0070] Users who select the data which they request for usage by means of menu or the introduction of contents request for the use of data M to the database 12 via a communication line 17 by the data communication apparatus 15.

[0071] At this time, the user encrypts by the public-key Kbd of the database 12 his own secret-key Ksu

$$Cksukbd=E\ (Kbd, Ksu)$$

and transmits it to the database 12.

[0072] The database 12 decrypts the encrypted secret-key Cksukbd of the user by the private-key Kvd

$$Ksu=D\ (Kvd, Cksukbd)$$

and encrypts the data M which is requested for use by the decrypted user secret-key Ksu

$$Cmksu=E\ (Ksu, M),$$

and transmits it to the communication apparatus 15 of the user via the communication line 17.

[0073] The user who receives the data Cmksu encrypted by own secret-key Ksu decrypts the encrypted data Cmksu with the user terminal 18

$$M=D\ (Ksu, Cmksu)$$

to use it.

[0074] This system is provided with charging center 13 which is incorporated within the database 12. This charging center 13 is used when the data is provided on a pay basis. In the case where the data is one which is provided for free such as shopping information or the like, this charging center 13 is not used. However, even if data are provided for free, such as shopping information or the like, the charging center is used in the case where charges are to be settled along with orders.

[Embodiment 2]

[0075] In the aforementioned embodiment, the public-key Kbd of the data managing center is broadcast from the broadcasting station instead of the communication line. Thus, it is impossible to confirm whether the public-key Kbd is justified or not.

[0076] In such a case, the private-key Kvd of the data managing center is used for digital signature to the public-key kbd of the data managing center.

$$Skbdkvd=E\ (Kvd, Kbd)$$

to be broadcast together with the public-key Kbd of the data managing center.

[0077] The user recognizes the digital signature Skbdkvd by the received public-key Kbd of the data managing center

$$Kbd=D\ (Kbd, Skbdkvd)$$

and when it is justified, uses the public-key.

[0078] Figs. 3(a) through 3(c) show modified exam-

ples which use a crypt key system according to the present invention.

[0079] To each example which has a structure as shown in figure 3 is applied the crypt key system, in electronic market transaction using the electronic data interchange system, to the credit settlement in retail shops shown in Fig. 3(a); the settlement by means of an electronic check shown in Fig. 3(b); and the wholesale conducted by makers and the like shown in Fig. 3(c).

[0080] In these systems, a digital signature is used in addition to the secret-key cryptosystem. These systems comprise a user 42, and a retail shop 43, a financial organization 44 or a wholesaler 45 such as a maker the like which is a World Wide Web (WWW) server on the internet.

[Embodiment 3]

[0081] In the credit settlement in the shop shown in Fig. 3(a), the shop 43 broadcasts data Ms such as an order form format, a credit card format, advertisements, catalogs, preview, products description, and content introduction of a database, and menu, charge schedule and price list, via the satellite 41 and a CATV line.

[0082] User 42 who receives the data Ms such as an order form format and a public-key Kbs of a shop 43 encrypts the user secret-key Ksu by the public-key Kbs of the shop 43

$$Cksukbs=E\ (Kbs, Ksu)$$

and enters Mu items such as the order content, the payment amount and a credit card number with encrypted by the secret-key Ksu of user 42 on the basis of information such as advertisement, catalog, products description and charges/prices list

$$Cmuksu=E\ (Ksu, Mu),$$

when needed, compresses Mu into a compressed document mu and signs digital signature by the private-key Kvu of the user 42

$$Smukvu=E\ (Kvu, mu),$$

and transmits it to shop 43 attached with the public-key Kbu of the user 42 via the network 47.

[0083] The shop 43 which has received the order decrypts the encrypted secret-key Cksukbs of the user 42 by the private-key Kvs of the shop 43

$$Ksu=D\ (Kvs, Cksukbs),$$

and decrypts the encrypted order document Cmuksu by the decrypted secret-key Ksu of the user 42

$$Mu=D\ (Ksu, Cmuksu).$$

[0084] Then, order acceptance is executed.

[0085] When the digital signature Smukvu is recognized by the public-key Kbu which the user 42 attached

$$mu=D\ (Kbu, Smukvu),$$

a receipt is sent to the user 42 via the network 47.

[0086] In this system, it is possible to prevent the unjustified use of the credit card number because the credit card number entered in the order form is sent encrypted.

[0087] Further, the following process enables reliable transaction:

[0088] The shop 43 compresses the digital data Ms1 of the order form format, the credit card format, advertisement, catalog, a preview, products description, and content introduction of the database and menu/charge schedule/price list into a compressed document ms1, with digital signature by the private-key Kvs of the shop 43

$$Smslkvs=E\ (Kvs, msl)$$

and broadcasts it attaching the public-key Kbs of the shop 43 so that users recognizes the digital signature Smslkvs by using the public-key kbs of the shop 43

$$ms'=D\ (Kbs, Smskvs).$$

[Embodiment 4]

[0089] In the settlement by means of electronic checks shown in Fig. 3(b), the bank as financial organization 44 broadcasts the blank check format Mf which is digital data attached with the public-key Kbf of the bank 44 via the satellite 41 or the CATV line.

[0090] The user 42 who receives the blank check format Mf encrypts the secret-key Ksu of the user 42 by the bank public-key Kb

$$Cksukbf=E\ (Kbf, Ksu),$$

enters Mu items concerning a payee and the payment amount with encrypted by the secret-key Ksu of the user 42

$$Cmksu=E\ (Ksu, Mu),$$

when needed, compresses Mu to the compressed doc-

ument mu, and sign by digital signature by using the private-key Kvu of the user 42

Smukvu=E (Kvu, mu)

and transmits them attaching the public-key Kbu of the user 42 and the encrypted secret-key Cksukbf of the user 42 which is encrypted by the public-key Kbf of the bank 44 to the bank 44 via the network 47.

[0091] The bank 44 which receives the described check uses the bank private-key Kvf to decrypt the encrypted secret-key Cksukbf of the user 42

Ksu=D (Kvf, Cksukbf),

decrypts the encrypted data Cmuksu of the payee and the payment amount by the decrypted user secret-key Ksu

Mu=D (Ksu, Cmuksu)

and recognizes the described content, and the currency exchange process is executed.

[0092] Furthermore, the bank recognizes the user 42 by Smuksu with the digital signature using the public-key Kbu added by the user 42

mu' =D (Kbu, Smuksu),

encrypts the confirmation document Ms2 by the public-key Kbu added by the user 42

Cms2kbu=E (Kbu, Ms2)

and sends it back to the user 42 via a network 47.

[0093] The user who receives the encrypted confirmation document Cms2kbu from the bank 44 decrypts the encrypted confirmation document Cms2kbu by the private-key Kvu of the user 42

Ms2=D (Kvu, Cms2kbu)

and confirms the content.

[0094] According to the system, since the party to which the payment is made and the payment amount are encrypted and described in the check, it is possible to prevent the unjustified use of the content described in the check.

[0095] In addition, the blank check format Mf which is digital data is compressed into a compressed document mf and signed by digital signature by using the private-key Kvf of the bank 44

Smfkvf=E (Kvf, mf)

to be broadcast attaching the public-key Kbf of the bank 44. The user recognizes the digital signature Smskvs by the public-key Kbs of the bank 44

mf'=D (Kbf, Smfkvf).

[0096] The confirmation document Ms is further compressed into a compressed document ms with digital signature by using the public-key Kbu added by the user

Smskbu=E (Kbu, ms)

[0097] Thus, the bank can recognize the user who has entered on the check.

[0098] In the systems shown in Figs. 3 (a) through 3 (c), since each format and advertisement with no need of secrecy are broadcast via satellite or CATV broadcasting, the data can be effectively transmitted.

[0099] As explained above, a multimedia system can be realized which combines general information media such as television broadcasting and audio broadcasting with data communication media using computers by using the crypt key system of the present invention, while the general information media and the data communication media has been existing so far as an independent system each.

[0100] A concrete structure for realizing the multimedia system will be explained as follows.

[0101] The current television broadcasting is provided by means of an analog system through terrestrial wave broadcasting, satellite broadcasting or CATV broadcasting. In the meantime, a most general data communication line is a public telephone line.

[0102] In such a system structure, the crypt key system according to embodiment 1 shown in Fig. 2 can be used as a basic structure of a system for realizing a video-on-demand. The broadcasting station broadcasts the public-key Kbb in multiplexing with the sub audio band of an audio zone in the scanning line of the vertical retrace interval of an analog television broadcasting program.

[0103] Users who wish to use the television program encrypt their own secret-key Ksu by the public-key Kbb broadcast from the broadcasting station

CKsukbb=E (Kbb, Ksu)

and request for the usage by transmitting the encrypted secret-key CKsukbb to the broadcasting station via a communication line.

[0104] The broadcasting station decrypts the encrypted secret-key CKsukbb of the users by the private-key

Kvb of the broadcasting station

ksu=D (Kvb, Cksukbb)

scrambles the broadcasting program by the decrypted secret-key Ksu and broadcasts it.

[0105] The users descramble the scrambled program for use by their own secret-key Ksu.

[0106] By adopting such a structure, persons other than users those who request to use the program cannot use the program.

[0107] Further, a crypt key system can be applied to television shopping which is frequently conducted currently by combining the television broadcasting and the telephone.

[0108] In the currently conducted television shopping which uses the analog television broadcasting, product introduction and sales method are presented on the television screen so that users record information on the sales method manually and request for the purchase thereof by a telephone on the basis of the recorded information.

[0109] In contrast thereto, the crypt key system according to the present invention proposes a transmission of data of the order format and the check format in multiplexing with the scanning line of the vertical retrace interval or the sub audio band of the audio zone.

[0110] In the meantime, an apparatus called personal computer television set which integrates a personal computer and a television set, or an apparatus which combines a video capture device which is realized as an IC card, a PC card or an insertion board and a personal computer, allows incorporation of the television picture.

[0111] With the combination of the multiplex data such as an order format and a check format with a video capture device, an electronic television shopping can be conducted.

[0112] In such a television shopping, when the television shopping product introduction display is broadcast, the order format and the check format are broadcast in data multiplex with the scanning line of the vertical retrace interval or the sub audio band of the audio zone.

[0113] If the users operate the apparatus when the product introduction display of the desired product to purchase is broadcast, the order format and the check format data are incorporated with the static display picture.

[0114] Users who wish to use the television shopping enter necessary items on the order format or check format to request for the purchase. To secure the safety of the transaction at this time, encryption by the public-key cryptosystem or the secret-key cryptosystem and digital signature are used with the system according to the embodiments of the present invention.

[0115] At this time, the content of transaction can be confirmed when the purchase order is requested by adding the static display picture of the product introduction together with the order and the check.

[0116] As a simple method, the order form format and the check format may be also transmitted as a television picture so that necessary items are entered on the order format and the check format which are incorporated as a static display picture.

[0117] In addition, the order form format and the check format can be transmitted via facsimile broadcasting which is multiplexed with the sub audio band of the audio zone.

[0118] By adopting such a method, an electronic market using electronic data interchange (EDI) by means of a current analog television method can be realized with the television shopping.

[0119] These video-on-demand system and pay-per-view system can be applied to the digital television broadcasting other than the analog television broadcasting.

[0120] Further, these video-on-demand system and pay-per-view system can be also applicable to transmission of high-quality audio data and moving picture data performed in computer communication network system using low-speed public telephone line or high-speed integrated services digital network (ISDN) or in internet system connecting a plurality of computer communication network.

[0121] As an apparatus to be used, the receiving apparatus and the communication apparatus can be incorporated in the television set. Apparatuses can be also constituted as a separate apparatus by using a set top box or the like.

[0122] In addition, a constitution with an apparatus referred to as a personal computer television set which is gradually prevalent, or an apparatus combining a video capture device, which is realized as an IC card a PC card or an insertion board for transmitting a television signal, to the personal computer, can be used.

Claims

1. A crypt key system comprising a broadcasting station (11), a database (12), a receiving apparatus (14), a data communication apparatus (15) and a user terminal (18), wherein
said database (12) and said broadcasting station (11) are connected with an online communication means, such as a dedicated line or the like, or an off-line means, such as a flexible disc or the like;
said database (12) and said data communication apparatus (15) are connected with a communication line (17);
said broadcasting station (11) and said receiving apparatus (14) are connected with a radio wave (16);
said receiving apparatus (14) and said user terminal (18) are connected with direct online means or with

off-line means, such as a flexible disc;
said data communication apparatus (15) and said user terminal (18) are connected with direct online means or with off-line means, such as a flexible disc;
said database (12) prepares a pair of a public-key and a private-key and supplies said public-key to said broadcasting station (11);
said broadcasting station (11) broadcasts said public-key;
said receiving apparatus (14) transmits said public-key, that has been received from said broadcasting station, to said user terminal (18);
said user terminal (18) stores said transmitted public-key;
said user terminal encrypts a secret-key of the user by said stored public-key and transmits said encrypted secret-key at the time of a request for data which the user desires, to said database (12) via said communication line (17); said database (12) which has received the request for data decrypts said encrypted secret-key of said user by said private-key, encrypts the data by said decrypted secret-key of said user and transmits the data to said data communication apparatus (15) via said communication line (17); and
said data communication apparatus (15) transmits the received data to said user terminal (18) which decrypts said data by said secret-key.

2. A crypt key system according to claim 1 wherein a digital signature of said database (12) is broadcast in addition to said public-key.

Patentansprüche

1. Verschlüsselungssystem mit einer Rundsendestation (11) einer Datenbank (12), einer Empfangsvorrichtung (14), einer Datenkommunikationsvorrichtung (15) und einem Benutzerendgerät (18), bei dem
die Datenbank (12) und die Rundsendestation (11) mit einer Online-Verbindungsvorrichtung wie einer ausschließlich zugeordneten Leitung oder dergleichen oder einer Offline-Vorrichtung wie einer flexiblen Scheibe oder dergleichen verbunden sind;
die Datenbank (12) und die Datenkommunikationsvorrichtung (15) mit einer Kommunikationsleitung (17) verbunden sind;
die Rundsendestation (11) und die Empfangsvorrichtung (14) durch eine Radiowelle (16) verbunden sind;
die Empfangsvorrichtung (14)und das Benutzerendgerät (18) mit einer direkten Online-Vorrichtung oder mit einer Offline-Vorrichtung wie einer flexiblen Scheibe verbunden sind;
die Datenkommunikationsvorrichtung (15) und das Benutzerendgerät (18) mit einer direkten Online-Vorrichtung oder mit einer Offline-Vorrichtung wie einer flexiblen Scheibe verbunden sind;
die Datenbank (12) ein Paar aus einem öffentlichen Schlüssel und einem privaten Schlüssel vorbereitet und den öffentlichen Schlüssel zu der Rundsendestation (11) liefert;
die Rundsendestation (11) den öffentlichen Schlüssel sendet;
die Empfangsvorrichtung (14) den öffentlichen Schlüssel, der von der Rundsendestation empfangen wurde, zu dem Benutzerendgerät (18) überträgt;
das Benutzerendgerät (18) den übertragenen öffentlichen Schlüssel speichert;
das Benutzerendgerät einen Geheimschlüssel des Benutzers durch den gespeicherten öffentlichen Schlüssel verschlüsselt und den verschlüsselten Geheimschlüssel zu der Zeit einer Anforderung von Daten, welche der Benutzer wünscht, über die Kommunikationsleitung (17) zu der Datenbank (12) überträgt;
die Datenbank (12), die die Anforderung von Daten empfangen hat, den verschlüsselten Geheimschlüssel des Benutzers durch den privaten Schlüssel entschlüsselt, die Daten durch den entschlüsselten Geheimschlüssel des Benutzers verschlüsselt und die Daten über die Kommunikationsleitung (17) zu der Datenkommunikationsvorrichtung (15) überträgt; und
die Datenkommunikationsvorrichtung (15) die empfangenen Daten zu dem Benutzerendgerät (18) überträgt, das die Daten durch den Geheimschlüssel entschlüsselt.

2. Verschlüsselungssystem nach Anspruch 1, bei dem eine digitale Unterschrift der Datenbank (12) zusätzlich zu dem öffentlichen Schlüssel durch Rundsendung übertragen wird.

Revendications

1. Système à clé de cryptage comprenant une station de radiodiffusion (11), une base de données (12), un appareil récepteur (14), un appareil de communication de données (15) et un terminal utilisateur (18), dans lequel
ladite base de données (12) et ladite station de radiodiffusion (11) sont connectées par un moyen de communication en ligne, tel qu'une ligne dédiée ou équivalent, ou un moyen autonome, tel qu'une disquette ou analogue ;
ladite base de données (12) et ledit appareil de communication de données (15) sont connectés par une ligne de communication (17) ;
ladite station de radiodiffusion (11) et ledit appareil récepteur (14) sont connectés par une onde radio

(16) ;
ledit appareil récepteur (14) et ledit terminal utilisateur (18) sont connectés par un moyen en ligne direct ou par un moyen autonome, tel qu'une disquette ;
ledit appareil de communication de données (15) et ledit terminal utilisateur (18) sont connectés par un moyen direct en ligne ou par un moyen autonome, tel qu'une disquette ;
ladite base de données (12) prépare une paire d'une clé publique et d'une clé privée, et fournit ladite clé publique à ladite station de radiodiffusion (11) ;
ladite station de radiodiffusion (11) émet ladite clé publique ;
ledit appareil récepteur (14) transmet ladite clé publique, qui a été reçue depuis ladite station de radiodiffusion, vers ledit terminal utilisateur (18) ;
ledit terminal utilisateur (18) stocke ladite clé publique transmise ;
ledit terminal utilisateur crypte une clé secrète de l'utilisateur par ladite clé publique stockée et transmet ladite clé secrète cryptée, au moment d'une demande de données que souhaite l'utilisateur, vers ladite base de données (12) via ladite ligne de communication (17) ;
ladite base de données (12), qui a reçu la demande de données, décrypte ladite clé secrète cryptée dudit utilisateur par ladite clé privée, crypte les données par ladite clé secrète décryptée dudit utilisateur, et transmet les données vers ledit appareil de communication de données (15) via ladite ligne de communication (17) ; et
ledit appareil de communication de données (15) transmet les données reçues vers ledit terminal utilisateur (18), qui décrypte lesdites données par ladite clé secrète.

2. Système à clé de cryptage selon la revendication 1, dans lequel une signature numérique de ladite base de données (12) est émise en plus de ladite clé publique.

FIG. 1

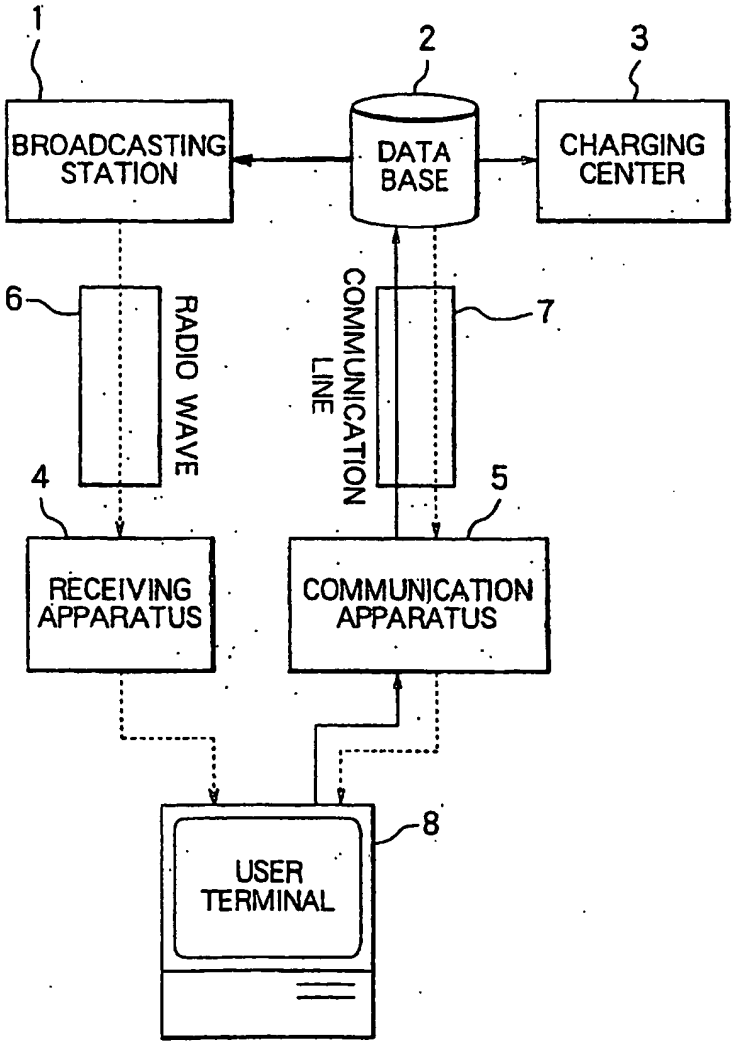
1
2
3
BROADCASTING STATION
DATA BASE
CHARGING CENTER
6
RADIO WAVE
COMMUNICATION LINE
7
4
5
RECEIVING APPARATUS
COMMUNICATION APPARATUS
8
USER TERMINAL

FIG. 2

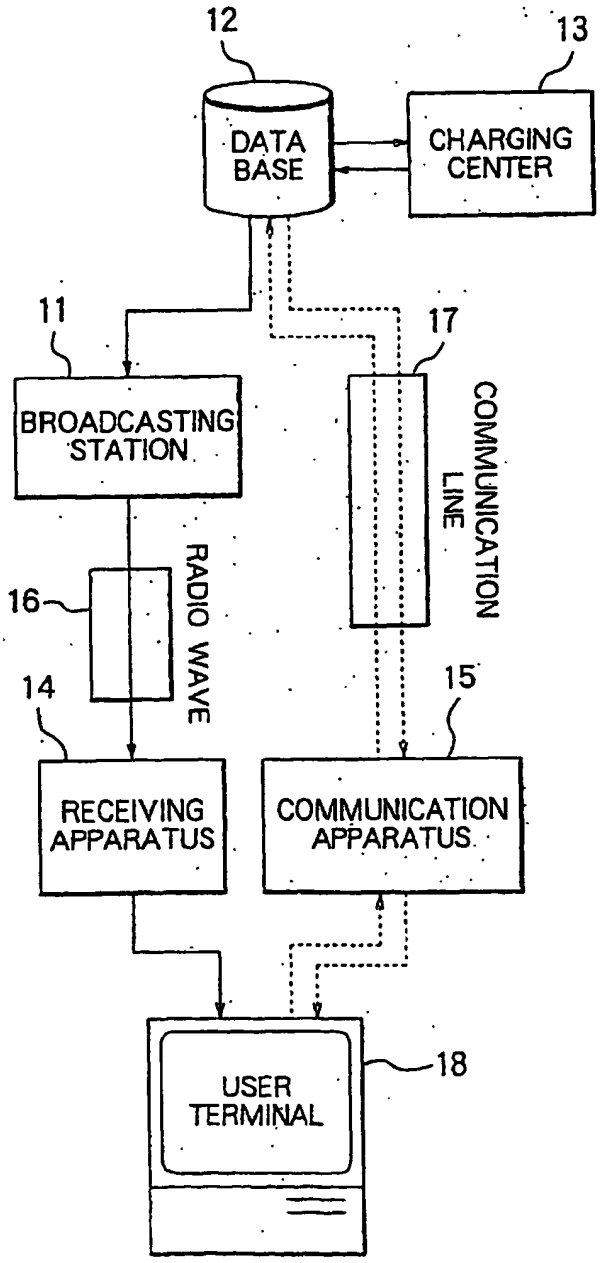
12
13
DATA BASE
CHARGING CENTER
11
17
BROADCASTING STATION
COMMUNICATION LINE
16
RADIO WAVE
14
15
RECEIVING APPARATUS
COMMUNICATION APPARATUS
USER TERMINAL
18

FIG. 3(a)

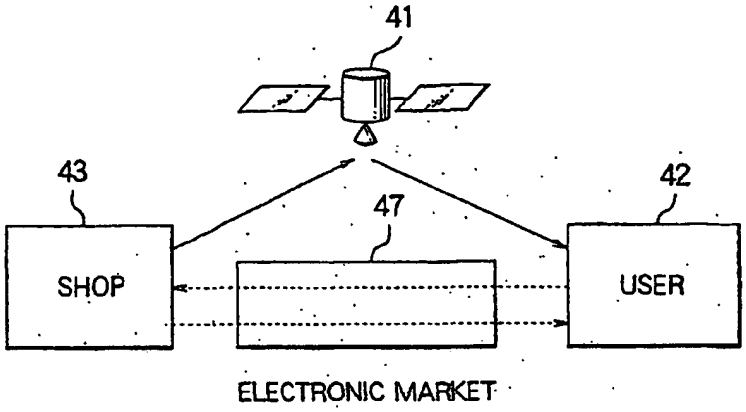

FIG. 3(b)

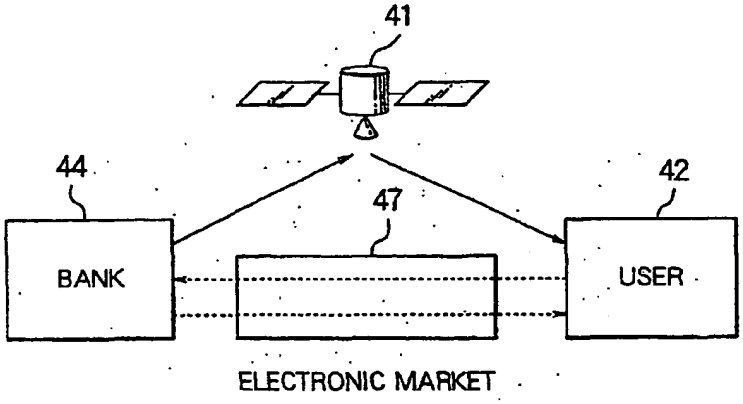

FIG. 3(c)